Case Western Reserve Law Review

Volume 52 | Issue 4

2002

Focusing on Infringement: Why Limitations on Decryption Technology Are Not the Solution to Policing Copyright

Brian Bolinger

COMMENTS

FOCUSING ON INFRINGEMENT: WHY LIMITATIONS ON DECRYPTION TECHNOLOGY ARE NOT THE SOLUTION TO POLICING COPYRIGHT

INTRODUCTION

J bn wfsz tvsqsjtfe uibu zpv xfou up uif uspvcmf pg efdjqifsjoh uijt qbsbhsbqi. Xijmf tjnqmf mfuufs tvctujuvujpo jt usjwjbmmz fbtz up csfbl, uif qspdftt pg fodpejoh boe efdpejoh uif mbohvbhf ifsf cz iboe jt ufejpvt bu cftu. Uif sftu pg uif Dpnnfou tipvme ibwf cffo fopvhi up vbso zpv uibu J eje opu ibwf bozuijoh jnqpsubou up tbz. Tpnf dpnnfoubupst ibwf tubufe uibu uif wbtu nbkpsjuz pg mbx sfwjfx bsujdmft bsf hjccfsjti.[1] J bn qspve up tubuf uibu, uispvhi uijt qbsbhsbqi, J ibwf qspwjefe uif gjstu mjufsbm fybnqmf pg uijt.

The above paragraph is a portion of this article that the author has chosen not to share with the casual reader of this article. If you desire access to the above material, it is required that you contact the Case Western Reserve Law Review for permission and the decryption process. You may decide it is not worth the effort to do so and simply ignore the opening paragraph. If so, you are now in the position of having lawfully obtained this copyrighted material yet without any way to access its content. You may instead decide to decipher the relatively simple encoding yourself and read the encoded text. Such an act would subject you to civil liability under United States ("U.S.") law.[2] An attempt to obtain the decryption key from a previous "licensee" of the Law Review would be equally problematic; both parties would be subject to liability in such a case.[3] In fact, there is presently no legal way to read the opening paragraph without first gaining the Law Review's permission.

---

[1] *See, e.g.*, Andrew J. McClurg, *The World's Greatest Law Review Article* (1995), *at* http://www.lawhaha.com/review_2.asp.

[2] *See* Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2000).

[3] *See id.*

The above example may seem ridiculous, but under the recently passed Digital Millennium Copyright Act ("DMCA"),[4] as a copyright owner, the Law Review has sweeping rights to control access to its copyrighted works, even for those possessing lawful copies of them. On March 6, 2002, the World Intellectual Property Organization ("WIPO") Copyright Treaty entered into force for the U.S. and twenty-nine other contracting nations.[5] The treaty was intended to update world copyright law in response to challenges presented by digital technology. Article 11 of this treaty requires each member nation to enact legislation to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights."[6] The DMCA represents the implementation of this statute under U.S. law.

The effects of Article 11 may be more extensive than was originally intended by the contracting nations. Already, Article 11 and its progeny have engendered a considerable amount of controversy, especially in the community of encryption researchers. The U.S., as the home of many of the largest producers of copyrighted works, was one of the driving forces behind the inclusion of Article 11 in the 1996 WIPO Copyright Treaty.[7] As a result, the DMCA has been the model for the laws of many of the contracting nations,[8] and a source of unease for citizens of a number of other nations.[9]

Given the strong influence of the DMCA in shaping international copyright law, Part I of this Comment conducts a detailed analysis of

---

[4] *Id.*

[5] *See* WIPO Press Release PR/2001/300, *30th Accession to Key Copyright Treaty Paves Way for Entry Into Force* (discussing briefly the history and significance of the treaty), *available at* http://www.wipo.org/pressroom/en/index.html (Dec. 6, 2001).

[6] *See* WIPO Copyright Treaty, Dec. 20, 1996, Art. 11, *reprinted in* PAUL GOLDSTEIN, INTERNATIONAL LEGAL MATERIALS ON INTELLECTUAL PROPERTY 177 (2000).

[7] *See* Peter Jaszi, *Taking the White Paper Seriously*, (noting that the U.S. submitted draft language for Art. 11), *available at* http://lcweb.loc.gov/nac/nac30/jaszi-1.html (last visited Mar. 6, 2002).

[8] *See, e.g.*, Copyright and Neighboring Rights Act, SG No. 28/2000 (2000) Art. 97(6) (Bulgarian criminal provision broadly prohibiting circumvention of protected works); Council Directive 2001/29, Art. 6(2), 2001 O.J. (L 167) (describing prohibited devices in terms similar to 17 U.S.C. 1201(a)(2)).

[9] *See, e.g.*, Niels Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results*, *at* http://www.macfergus.com /niels/dmca/cia.html (Aug. 15, 2001) (explaining the reluctance of a Dutch cryptographer to publish his work for fear of liability under the DMCA); Denis Kelleher, *Confusion Over Copyright and Free Speech*, THE IRISH TIMES (Aug. 27, 2001) (expressing author's fear that a U.S. disregard for free speech rights in computer programs might set a poor precedent for the European Community) *available at* http://www.ireland.com/ newspaper/computimes/2001/0827/comp2.htm; Anand Parthasarathy, *Clash of Cryptography and Copyright*, THE HINDU (Sept. 13, 2001) (expressing concern over the breadth and international reach of the DMCA) *available at* http://www.hindunet.com/thehindu/2001/09/13/stories/ 0813009. htm.

the statute and its likely effects on encryption research. Part II considers the general consequences of granting exceptional protection to encryption processes as incident to the copyright of an underlying work. Such protection constitutes a new, unique species of intellectual property and a sharp departure from the traditional limitations placed on intellectual property monopolies under U.S. law. Finally, Part III presents alternative models for providing protection to technologically protected works.

I. THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. The Anti-Circumvention Provisions

Under § 1201(a) of the DMCA,[10] no person may "circumvent a technological measure that effectively controls access to a work protected under [U.S. copyright law]."[11] To circumvent a technological measure is broadly defined as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[12] The definition of effective control is equally broad; a technological measure 'effectively controls access to a work' if, "in the ordinary course of its operation, [it] requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[13]

Unfortunately, the statute does not make clear what the term "technological measure" signifies. It might be assumed that as a part of the DMCA, the anti-circumvention provision applies only to digital measures, but further prohibitions within § 1201 apply solely to analog devices,[14] casting doubt on this argument. *Webster's New World Dictionary* defines technical as "having to do with the useful or industrial arts or skills."[15] Under this definition, a technological measure could be literally anything that restricts access to the work, even the mechanically applied shrink wrap on the outside of a compact disc ("CD") or digital versatile discs ("DVD"). At least one court has stated in dicta that "the statute is clear that it prohibits '*any technology*,' not simply black boxes."[16]

---

[10] 17 U.S.C. § 1201 (2000).
[11] *Id.* § 1201(a)(1)(A).
[12] *Id.* § 1201(a)(3)(A).
[13] *Id.* § 1201(a)(3)(B).
[14] *See id.* § 1201(k).
[15] WEBSTER'S NEW WORLD DICTIONARY: BASIC SCHOOL EDITION 764 (Southwestern Co. 1984).
[16] Universal City Studios v. Reimerdes, Inc., 111 F. Supp. 2d 294, 317 n.135 (S.D.N.Y. 2000).

Given the context of the statute, however, it would seem likely that the "technological measures" discussed in § 1201 would be restricted to encryption measures, scrambling systems, and similar protective devices. The legislative record bears out this theory, stating that the coverage under the statute would be limited to "measures that would be deemed to effectively control access to a work would be those based on encryption, scrambling, authentication, or some other measures which requires the use of a 'key' provided by a copyright owner to gain access to a work."[17]

The question remains, however, how effective a protective measure must be to gain protection under the statute. There is no requirement under the statute that the measure be novel or meet certain standards of effectiveness. Accordingly, it appears that literally any attempt at encryption by a copyright owner, even through use of a technique in the public domain, garners protection under the statute. At least one court has found that the strength of an encryption method is irrelevant in determining its protection under the DMCA.[18] Under this ruling, even the simplistic coding used in the opening paragraph of this Comment qualifies for protection.

In § 1201(a)(2) and § 1201(b), the DMCA further prohibits the "manufactur[ing], import[ing], offer[ing] to the public, provi[ding], or otherwise [trafficking] in any technology, product, service, device, component, or part thereof,"[19] falling within three categories. Before turning to the individual categories, it is worth mentioning the "or part thereof" language contained within this provision. This provision does not just apply to specific circumvention devices, but literally to "any part" of the decryption technology. Neither the statute nor the case law makes clear precisely how far this "any part" language may extend. The bare language, however, would extend the publication of information about the encryption theory used within a particular measure. Courts have shown a willingness to interpret the provision broadly. For example, the bare, uncompiled source code of a decryption program has been found to fall within the terms of the statute.[20] Would suggesting the vulnerability of a particular encryption scheme to brute force decryption within the context of an article constitute publicizing "a part" of a decryption technology? Until this

---

[17] 144 CONG. REC. E2136, 2137 (1998) (statement of Rep. Bliley).

[18] *See Universal City Studios*, 111 F. Supp. 2d at 318 (citing RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000)) (stating that a method that otherwise meets statutory requirements falls under the statute regardless of whether it is a "strong means of protection").

[19] 17 U.S.C. § 1201(a)(2), §1201(b)(1) (2000).

[20] *See Universal City Studios*, 111 F. Supp. 2d at 346 (holding that DMCA applies to technology that circumvents the protection system of digital versatile disks).

question, and others like it, is answered, the DMCA will have a chilling effect on speech and research within the field of cryptography.

Returning to the protected categories under the provision, the first concerns devices "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [U.S. copyright law]."[21] Thus, any device, no matter how it is manufactured (i.e., reverse engineering, or independent discovery of an encryption method), which is designed primarily to allow access to protected works, may not be manufactured or sold without the permission of the copyright owner utilizing the encryption. The implications of this will be discussed further below.[22]

A second category of prohibited devices encompasses devices "marketed by [the provider of the device] or another acting in concert with [the provider] with [the provider's] knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [U.S. copyright law]."[23] This provision allows copyright owners to bring suit against anyone within the chain of distribution so long as their marketing techniques indicate knowledge of the circumvention function of the product. Practically speaking, it allows the copyright owner who finds a circumvention device for sale that applies to her product to both save the expense of tracking down the actual creator of the device and seek out the proverbial "deep pocket" within the chain of distribution. It should be noted that under this provision, neither the purpose of the design of the device, nor any significant commercial purposes it may possess are relevant in determining a violation of the statute. It is only necessary that it be marketed for use in circumventing access control measures protected under the statute, and that a person "trafficking" in the device be aware of this.

Given that at least one court has broadly defined trafficking to include merely creating a hypertext link to a file,[24] this provision could implicate a number of seemingly legitimate activities. Under such a standard, linking to a site offering to sell a cryptography text claiming to demonstrate the shortcomings of a particular encryption system may incur liability under this statute.

Finally, the third protected category covers devices that have "only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to

---

[21] 17 U.S.C. § 1201(a)(2)(A) (2000).

[22] *See infra* Part II.B.

[23] 17 U.S.C. § 1201(a)(2)(C) (2000).

[24] *See Universal City Studios*, 111 F. Supp. 2d at 303, 346.

a work protected under [U.S. copyright law]."[25] It should be noted here that this provision affects any part of a decryption technology that cannot be put to a significant commercial use. The statute is not clear as to what constitutes a commercial use, but in the context of fair use, at least, courts have defined "commercial use" broadly.[26] Consequently, articles, web page content, and encryption research could possess a commercial use beyond their use in circumventing access control measures.

B. Permitted Circumvention

In response to the broad sweep of the § 1201(a) and § 1201(b) prohibitions, Congress included a number of narrow exceptions within the statute. One narrow exception is limited to nonprofit libraries, archives, and educational institutions.[27] This exception merely protects an institution's decryption of a work in violation of § 1201(a) in a good faith attempt to determine if it wishes to purchase a work.[28] The exception does not apply where the institution can reasonably access the work in another manner, and even where applicable, the work may only be retained for a sufficient time to allow the institution to evaluate the work.[29] A broader exemption protects government entities and their officials acting in the scope of their duties.[30] Neither exception is significant in limiting the DMCA's intrusion on the public domain.

Section 1201 also contains a limited exception for reverse engineering.[31] A person who "has lawfully obtained" rights of use for a computer program may circumvent an access control measure without liability under § 1201(a) or § 1201(b) under limited circumstances.[32] Specifically, the individual may obtain access to analyze "those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs."[33] The statute defines interoperability as "the ability of computer programs to exchange information, and to share the information which

---

[25] 17 U.S.C. § 1201(a)(2)(B) (2000).

[26] *See, e.g.*, Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 914 (2d Cir. 1994) (defining commercial use to extend to the photocopying of eight articles in a scientific journal for use by a researcher); A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000) (defining commercial use to include providing a "peer-to-peer file-sharing system that allows users to conduct music file searches on other computer hard drives").

[27] 17 U.S.C. § 1201(d) (2000).

[28] *Id.*

[29] *Id.*

[30] *Id.* § 1201(e).

[31] *Id.* § 1201(f).

[32] *Id.*

[33] *Id.* § 1201(f)(1).

has been exchanged."[34] This exception applies only if the individual did not already have access to the elements of interest prior to the circumvention. Further, it provides a defense only to the anti-circumvention provisions; the individual is still liable for any infringing acts in ensuring interoperability. Information gained and technology developed can only be shared with others to the extent it is necessary to ensure the interoperability of the independently created program with other programs.[35]

Despite the broad wording, this exception remains fairly narrow. The main limitation lies in the fact that the exception applies solely to computer programs. There is no indication that the term "computer program" includes digital data. In fact, a recent district court decision specifically rules that the provision does not extend to such data.[36] While an individual adapting a program to a particular computer operating system might be protected, an individual independently developing a DVD player would remain liable under § 1201(a) & (b). Further, this statute does not protect reverse engineering, a program to create a rival program or even for intellectual curiosity, but only for purposes of interoperability. This greatly restricts the range of programs that may be subject to this exception.

Another exception exists for encryption research, defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works."[37] Such activities may only qualify under the statute if they "are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[38] This definition is sufficiently broad; if all encryption research were allowable, the statute would have little effect on such activities. Unfortunately, not all the activities traditionally associated with encryption research are exempted under the statute.

The statute lists several factors to be considered on whether a defense of encryption research may exempt a researcher under the statute. First, a researcher is encouraged to promptly notify the copyright owner of any results of his of her research.[39] Although sharing one's results with the party most affected by them is reasonable given the general policy goal of improving and strengthening encryption techniques, under the present state of the law, such an action is tanta-

---

[34] *Id.* § 1201(f)(2).

[35] *See id.*

[36] Universal City Studios, Inc. v. Reimerdes Inc., 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (holding that DMCA applies to technology that circumvents the protection system of DVD).

[37] 17 U.S.C. § 1201(g) (2000).

[38] *Id.* § 1201(g)(1)(A).

[39] *See id.* § 1201(g)(3)(C).

mount to an invitation to be sued. Accordingly, this factor may be less indicative of the intent of the researcher than it is of the aggressiveness of the legal department of the copyright owner. Second, the court must consider whether the researcher is employed or trained in the field of cryptography.[40] This factor might discourage work by amateur or hobbyist cryptographers who lack formal credentials, but it is only one factor to be considered. It certainly seems fair to at least consider the prior work and training of those claiming to advance the state of cryptography.

Finally, the court must factor in the manner of distribution of the results of the research. Specifically, the court must determine if they have been distributed "in a manner reasonably calculated to advance the state of . . . encryption technology, [or] . . . in a manner that facilitates infringement under this title or a violation of [other] applicable law."[41] Under this factor, it would appear that publishing one's work in a peer-reviewed journal would be a strong indication that research was performed in the proper manner. As discussed below, however, the very act of publishing the article may not be protected under the exception.

Assuming the researcher prevails in the above analysis, the encryption research exception exempts encryption researchers from liability under § 1201(a) for circumventing access control measures on copyrighted works, subject to four conditions. Two of these are quite obvious; the encrypted copy must be legally obtained,[42] and the decryption cannot constitute copyright infringement itself or otherwise violate other federal law.[43] The others, however, are somewhat vague. For example, the circumvention must be necessary for the researcher to conduct his encryption research.[44] The problem with this apparently innocuous little clause lies in the fact that the exemption is an affirmative defense under the statute.[45] The researcher bears the burden of showing that his actions were necessary.

While showing that the decryption action was necessary to further encryption research does not seem like a heavy burden, no court has yet passed upon the meaning of "necessary" under the statute. Hence, it could mean anything from a simple statement that only research related decryption will be permitted to a threat of liability for researchers unfortunate enough to overlook an alternate source for the information. To pose a ridiculous example, a researcher circumvent-

---

[40] *See id.* § 1201(g)(3)(B).
[41] *Id.* § 1201(g)(3)(A).
[42] *See id.* § 1201(g)(2)(A).
[43] *See id.* § 1201(g)(2)(D).
[44] *See id.* § 1201(g)(2)(B).
[45] *See id.* § 1201(g)(2).

ing access control measures on a DVD copy of the cartoon of *Bambi* could have used a *Snow White* DVD using the same measures instead. Thus, it was not strictly necessary to circumvent the access controls on that *Bambi* when *Snow White* was available. A more plausible example might be found in education; is it "necessary" for students to tackle encryption schemes that have already been broken to strengthen their grasp of the theory? If a researcher has reason to believe that two encryption schemes are similar, is it "necessary" to circumvent the first to better understand the second? While I believe that any court would find the above three examples sufficient to constitute necessity, I am not staking my reputation, my financial comfort, or my freedom on the result. An encryption researcher performing the research is risking all three with the initiation of each new project.[46] Even if a researcher were sure that she had complied with the requirements of the statute, it is unlikely she would wish to expend the time or money to be the test case for defining "necessary" under the statute.

The final requirement for the encryption research exception requires the researcher to make a good faith effort to obtain permission from the copyright owner prior to decrypting the work.[47] Even assuming that no difficulties arise in determining the copyright owner of the underlying work, given the breadth of the DMCA, few researchers will wish to call the attention of major copyright holders to their research before it is even commenced. Such a request for permission is likely to be answered with a "cease and desist" letter; copyright owners have little to gain in allowing their access control measures to be broken. Although copyright owners have shown some willingness to work with researchers in the past, they have shown an equal willingness to ensure that research on their product is performed on their terms.[48] This raises what is perhaps the most troublesome question raised by the requirement; if a copyright owner grants permission to a researcher subject to terms such as a ban on publication or other secrecy requirements, must the researcher accept the terms to meet the good faith requirement? How onerous can these terms be? If this issue is not litigated in the case of Professor Felten,[49] it almost certainly will be within the next few years. Again, no researcher will be eager to become the test case for this issue, chilling their work until its resolution.

---

[46] *See* 17 U.S.C. § 1203 (2000) (imposing civil liability for willful violations of anti-circumvention provisions); 17 U.S.C. § 1204 (2000) (imposing criminal liability for violations of anti-circumvention provisions).

[47] *See* 17 U.S.C. § 1201(g)(2)(C) (2000).

[48] *See infra* Part I.C, notes 55-56.

[49] *See id.*

It should be noted that even where a researcher desiring to publish his or her work qualifies for the research exception, the exception applies only to violations under § 1201(a). Therefore, even a bona fide encryption researcher may be subject to liability under § 1201(b) upon publishing for making available to the public a part of a technology primarily designed to circumvent an access control measure. Although the language in § 1201(b) is virtually identical to the language of §§ 1201(a)(2) and (3), the research exception applies only to the former. Until this particular difficulty is resolved, it is unlikely that a researcher will be confident in relying on this provision.

Another exception allows circumvention of access control measures on protected works when either the access control measures or the protected work collect personal information about the user seeking access without giving the user notification and an opportunity to opt out of the collection.[50] Given the unfortunate trend of software distributors to include such capabilities in their works,[51] this exception is necessary to protect the privacy of copyright users. Unfortunately, it does little to alleviate the problems discussed earlier.

The statue also contains an exception for bona fide security testing of a computer.[52] The language of this exception is quite similar to that of the encryption research exception, with many of the same shortcomings. Like the encryption exception, this exception does not apply to § 1201(b), making it illegal to disseminate the results of even bona fide testing.[53] Unlike encryption research, however, the need for publication of security testing results is not as vital. While publication of the results can forewarn users of a program of its vulnerabilities, they can just as easily facilitate attacks on these systems. Thus, the failure to provide a dissemination exception here may be the wisest course of action under the statute.

C. International Effects of the DMCA

Even in those countries that have not ratified the WIPO Copyright Treaty, its terms may have a chilling effect on programmers and encryption researchers. For example, nothing in the DMCA restricts its civil or criminal penalties to American citizens. In fact, the first

---

[50] 17 U.S.C. § 1201(i) (2000).

[51] *See e.g.*, Rothken Law Firm Press Release, *Fahrenheit Entertainment and Sunncomm are Sued for Violating Privacy Rights of California Consumers and for Unfair Business Practices, available at* http://www.techfirm.com/mcrel.pdf (Sept. 6, 2001); Sara Robinson, *CD Software Is Said to Gather Data on Users*, N.Y. TIMES ABSTRACTS (Nov. 1, 1999), *available at* 1999 WL30547639.

[52] 17 U.S.C. § 1201(j) (2000).

[53] *See id.*

criminal prosecution instituted under the statute was brought against a Russian national for acts committed while still in Russia.[54]

In a widely publicized case, the U.S. Department of Justice brought charges against a Russian programmer, Dmitri Sklyarov, for his participation in the creation and distribution of a decryption program known as the Advanced eBook Processor for his employer ElcomSoft.[55] The Advanced eBook Processor allows a user to transform eBooks in the proprietary Adobe eBook format into an ordinary .pdf file. All of Sklyarov's work on the program and all of the business related to its distribution were carried out in his native Russia. His arrest took place while he was giving a talk in Las Vegas. The complaint filed by the Department of Justice, although not directly addressing jurisdictional issues, seems to have based jurisdiction on a single sale of the Advanced eBook Processor to an Adobe executive.[56]

Sklyarov was finally released after a substantial wave of protest over his detainment. His arrest, however, opens substantial questions over the intended breadth of the DMCA. Under customary international law, a nation may exercise jurisdiction over any act taking place in its territory. Given the ubiquitous nature of the Internet, however, any significant commercial distribution of a software product will almost always take place, at least in part, within the territory of the United States. This extends the reach of the statute to anyone who visits the United States. Given the rapid spread of anti-circumvention law intended to comply with Article 11, soon, internet publishers and distributors will be reluctant to leave their home country for fear of being subjected to one of a number of broadly worded paracopyright laws.

A prime example of this very fear is illustrated by the case of Niels Ferguson, a prominent Dutch cryptography expert. Ferguson's research has revealed a major flaw in Intel's encryption scheme for firewall connections, the High-Bandwidth Digital Content Protection System ("HBCP").[57] Ferguson, however, refuses to publish his results for fear of liability under the DMCA.[58] In his own words, "I travel to the US regularly, both for professional and for personal reasons. I simply cannot afford to be sued or prosecuted in the US. I

---

[54] *See* Editorial, *Jailed Under a Bad Law*, WASH. POST (Aug. 21, 2001), *available at* http://www.washingtonpost.com/ac2/wpdyn?pagename=article&node=opinion&contentId=A38463-2001Aug20&notFound=true.

[55] *See id.*

[56] *See* Affidavit of Daniel J. O'Connell for Complaint at ¶ 8, United States v. Sklyarov, (N.D. Cal. July 7, 2001) (No. 5-01-257) (alleging that an Adobe employee purchased a copy of the Elcomsoft unlocking software over the Internet).

[57] *See* Ferguson, *supra* note 9.

[58] *See id.*

would go bankrupt just paying for my lawyers."[59] Other cryptography experts have also withdrawn their work from publication, citing similar concerns.[60]

Although Ferguson's reaction may seem extreme, there is unfortunately ample precedent to justify his concerns. A well-publicized example can be found in the difficulties experienced by Dr. Edward Felten and his colleagues in their attempt to publish a similar paper.[61] Dr. Felten and his colleagues were participants in an open challenge issued by The Secure Digital Music Initiative Foundation ("SDMI") to cryptographic researchers and hackers to break a number of proposed copy control measures implemented by SDMI.[62] SDMI provided each participant with samples for each of a number of technologies subject to a limited license agreement.[63] SDMI also provided a means for participants to check their solutions.[64] For each successful answer, SDMI offered successful researchers $10,000 for their research results.[65] Dr. Felten and his colleagues turned down the offer, and instead retained rights to their research in accordance with the license agreement.[66] Dr. Felten planned to publish his findings at an encryption conference, but when his role in the conference was publicized, SDMI responded with a cease and desist letter to both Dr. Felten and the conference itself.[67] Facing a lawsuit, the conference declined to allow the presentation of Felten's paper.[68] Dr. Felten and his colleagues were forced to bring an action for declaratory judgment to ensure their right to publish their results.[69]

II. A FOCUS ON PROTECTING TECHNOLOGICAL PROTECTION MEASURES GREATLY INCREASES THE SCOPE OF THE INTELLECTUAL PROPERTY MONOPOLY

The protections offered by Article 11 do not fall within the rubric of copyright law. Article 11 protects encryption techniques directly as processes, not indirectly through their underlying code as an

---

[59] *Id.*

[60] *See, e.g.*, Brian McWilliams, *Security Expert's DMCA Protest Rallies Supporters*, WASH. POST (Sept. 6, 2001) (discussing Dug Song's withdrawal of his cryptography information from his website), *available at* http://www.newsbytes.com/news/01/169829.html.

[61] *See EFF: Scientists Support Professor's Copyright Law Challenge*, *at* http://www.newsforge.com/article.pl?sid=01/08/14/0131222&mode=nocomment (Aug. 13, 2001).

[62] *See id.*

[63] *See id.*

[64] *See id.*

[65] *See id.*

[66] *See id.*

[67] *See id.*

[68] *See id.*

[69] *See id.*

original work of authorship. Such protections have been more appropriately referred to as paracopyright;[70] instead of directly protecting the rights granted to an author under the copyright provisions, anti-circumvention provisions create rights incident to a copyright. These ancillary rights are meant solely to grant copyright owners more leverage in enforcing their copyright. Even one of the authors of the DMCA acknowledges that the bill cannot be properly based upon the Copyright Clause of the Constitution.[71]

A. The DMCA Extends Copyright Protection to Encryption Processes

Statutes such as the DMCA grant copyright owners unprecedented intellectual property rights in the access control measures protecting their works. To receive its protection, the DMCA requires only that an access control measure "effectively controls access" to a protected work.[72] This standard is met by any measure which, "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[73] There is no standard of novelty that must be shown to receive this protection. Accordingly, even though the statute extends this protection to processes, traditionally beyond the bounds of copyright law,[74] it lacks the controls found in patent law that limit the withdrawal of processes from the public domain.

Focusing on U.S. intellectual property law, the scope of protection granted anti-circumvention measures under the DMCA appears similar to that granted for a trade secret. The statute protects access control measures from misappropriation by outside parties. It does not explicitly prevent others from independently practicing the protected method. On its face, the DMCA merely extends federal protection to subject matter already protected by state trade secret laws. Two important differences, however, expand the scope of protection granted by the DMCA well beyond that of prior law.

The first, and most obvious, difference lies in the definition of circumvention. Basically, any attempt to gain access to the content of a protected work is prohibited, if it is done "without the authority of

---

[70] *See* 144 CONG. REC. E2136, 2137 (1998) (discussing paracopyright as an area of regulation that covers activities falling outside the intellectual property realm).

[71] *See id.* at 2136 (discussing how the Copyright Clause is traditionally used to regulate "the use of information—not the devices . . . by which the information is delivered").

[72] 17 U.S.C. § 1201(a)(2)(A) (2000).

[73] *Id.* § 1201(a)(3)(B).

[74] *See* 17 U.S.C. § 102(b) (2000) (stating that copyright protection does not extend to such measures).

the copyright owner."[75] State trade secret laws typically require some form of misappropriation of a trade secret to create liability.[76] The ordinary trade secret case invariably involves employee misconduct or some immoral or illegal act by the competition. A competitor or even a third party who gains access to a trade secret by innocent means can generally practice or publish the trade secret without repercussion.[77] The cliché example of this is the hypothetical of the man walking by the headquarters of Coca-Cola® and picking up a piece of paper off of the sidewalk with the famous recipe for Coke® written upon it. Few state laws will prevent the man from doing as he wishes with the formally secret formula, as trade secret protection dissipates when the secret leaves its owner's control.

Under the DMCA, however, such innocent discovery does not destroy protection. If the secret cola formula in the above hypothetical is replaced with encryption keys or source code relating to a DVD encryption scheme, its finder must now take great care in how he treats the information. He cannot, for example, use the discovered encryption keys to watch his legally owned DVD on a non-compliant player, as this would circumvent an access control measure without the authorization of the copyright owner.[78] He would be further prohibited from publishing the material or showing it to a friend with an interest in cryptography.[79] To take an extreme example, under a literal interpretation of the statute, our hypothetical finder could be subjected to liability even for merely returning the slip of paper to the sidewalk upon which he found it, as this could be interpreted as providing the work to the public.

While the above example provides a trivial case, the DMCA also prevents a more substantial variety of innocent discovery, reverse engineering. Traditionally, trade secret law did not protect the use of a lawfully obtained sample of a product to determine its composition or method of manufacture.[80] This provides a significant limitation on trade secret law; although protection was easily obtained and theoretically infinite in duration, it could not prevent a product from reveal-

---

[75] 17 U.S.C. § 1201(a)(3)(A) (2000).

[76] *See* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015 (5th Cir. 1970) (holding that aerial photography of a competitor's plant construction is actionable misappropriation of a trade secret).

[77] *See* Vacco Indus. v. Van den Burg, 6 Cal. Rptr. 2d 602, 611 (Ct. App. 1992) (noting that trade secret protection rests upon the theory of improper acquisition).

[78] *See* 17 U.S.C. § 1201(a)(1) (2000).

[79] *See id.* § 1201(a)(2).

[80] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (stating that trade secret law doesn't protect "against discovery by fair and honest means" such as "independent intervention" or "accidental disclosure").

ing its secrets once it had reached the market. Accordingly, the protected information would eventually enter the public domain.

Processes protected under the DMCA, however, can never enter the public domain unless they are abandoned by the copyright owner. With limited exceptions, reverse engineering of access control measures protected by the DMCA is prohibited.[81] Even if by some accident information relating to the access control measure is lawfully obtained, the DMCA prevents public distribution or use of the information.[82] Like the holder of a patent, a copyright owner protecting an access control measure under the DMCA can prevent the unauthorized use of its encryption methods. This protection, however, is of limited duration and is not circumscribed by a claim to outline the limits of the protection. In this respect, the protection granted to these encryption programs is significantly greater than that granted to the circuitry used to implement them. Allowing this degree of protection over unproven encryption schemes would significantly retard progress within the field.

B. The DMCA Extends Copyright Protection to Devices Related to the Copyrighted Work

A focus on protecting access control measures will also invariably lead to the inclusion of devices utilizing the copyrighted work within the copyright monopoly. Specifically, so long as the copyright owner has the sole power to grant access to a protected work, any related device intended to provide access to the work falls under the control of the copyright owner. While an individual copyright owner has little power to affect the market for such goods, large copyright owners, working in tandem, can easily extend their access control rights to control the production of any such licensed goods. Unfortunately, this is not mere speculation; major copyright owners in the U.S. have already formed similar organizations to ensure the licensing of playback devices. Examples include the DVD Copy Control Association and the Secure Digital Music Initiative, formed by the major copyright holders in the video and audio industries.

While copyright owners could attempt such control without extensive legal protection of access control measures, their bargaining position in licensing such measures would be sharply curtailed. In the absence of access control measures, any prospective manufacturer could develop its own circumvention method to create a playback device. If nothing else, a manufacturer could reverse engineer an ex-

---

[81] *See* 17 U.S.C. § 1201(f) (2000).

[82] *See supra* notes 30-32 and accompanying text.

isting system to gain the necessary encryption algorithms. Accordingly, the cost of a license from the copyright owners would never exceed the cost of independent development of a decryption system. Thus, providing direct protection of access control measures constitutes a gift to copyright owners of the value of playback devices and other devices related to the use of their copyrighted works.

There has always been a conflict in U.S. intellectual property law between the desire to encourage and reward creativity and the fear of granting monopoly power. U.S. law has always sharply limited the scope of granted monopolies over intellectual property. Any attempt to expand an intellectual property monopoly beyond these carefully defined domains violates the purpose of intellectual property law; the increase of new ideas in public discourse. As Justice Stevens once observed, Congress views its role in enacting a copyright law as follows, "Congress must consider . . . two questions: First, how much will the legislation stimulate the producer and so benefit the public; and, second, how much will the monopoly granted be detrimental to the public?"[83] Any extension of intellectual property rights is reasonable only so far as it works to enrich the public domain.

This viewpoint, while not unique to U.S. law, is not necessarily the norm. In many European countries, intellectual property rights, especially copyright, are considered the automatic property of their creator, his or hers by moral right. U.S. intellectual property law rejects this theory. The U.S. recognizes only limited moral rights in copyrighted works.[84] Intellectual property rights are granted solely by the mandate of the U.S. Constitution only to further the development of the useful arts.[85] It is nothing but a bribe for the talented, meant to encourage the free flow of ideas to the public.

The U.S. common law aversion to extension of the intellectual property monopoly finds its voice in the doctrines of patent and copyright misuse. American courts have responded to attempts to extend the monopoly granted to a protected work by temporarily negating the granted protection.[86] For example, a copyright or patent holder is

---

[83] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 429 n.10 (1984) (quoting H. R. REP. NO. 2222, at 7 (1909)).

[84] *See* 17 U.S.C. § 106A (2000) (stating that one has a right to "claim authorship" of one's work).

[85] *See, e.g., Sony Corp.*, 464 U.S. at 429 n.10 (opining that "[t]he enactment of copyright legislation by Congress under the terms of the Constitution is not based upon any natural right that the author has in his writings, . . . but upon the ground that the welfare of the public will be served and progress of science and useful arts will be promoted by securing to authors for limited periods the exclusive rights to their writings") (quoting H. R. REP. NO. 2222, at 7 (1909)).

[86] *See* Eastman Kodak Co. v. Image Technical Servs., 504 U.S. 451 (1992); Lasercomb America, Inc. v. Reynolds, 911 F.2d 970, 979 (4th Cir. 1990) (holding that a copyright owner was barred from suing for copyright infringement where it had misused the copyright).

prohibited from including anticompetitive clauses in standard licensing agreements[87] or attempting to control the market for staple articles of commerce related to the product.[88] So long as he or she attempts to do so, the court will not enforce their intellectual property rights.[89]

The Fifth Circuit's decision in *Alcatel USA, Inc. v. DGI Technolgies, Inc.*[90] illustrates the reluctance of U.S. courts to extend the copyright monopoly to related devices. DGI Technologies was found to have infringed upon Alcatel's copyright in its software in developing a microprocessor for a telephone switching system compatible with Alcatel software. The court of appeals, however, vacated the injunction granted by the trial court, finding that Alcatel had misused the copyright over its software in attempting to extend its protection to its unpatented microprocessor. In accepting the doctrine of copyright misuse, the court observed that "whereas 'copyright law [seeks] to increase the store of human knowledge and arts by rewarding . . . authors with the exclusive rights to their works for a limited time . . . , the granted monopoly power does not extend to property not covered by the . . . copyright.'"[91] Unfortunately, under the DMCA, the limits of the monopoly grant will no longer be so sharply defined. Material more properly the subject of trade secret or patent can now be legally tied to a copyrighted work, but is tied by statute, so long as it contains a minimally effective access control measure.

III. ALTERNATIVE MODELS FOR DETERRING MASS COPYRIGHT INFRINGEMENT IN THE DIGITAL AGE

A. Limit the Scope of Anti-Circumvention Statutes to Prevent Excessive Encroachment on the Public Domain and Scientific Discourse

Not all anti-encryption statutes are as restrictive as the DMCA. Perhaps the best statute compatible with obligations under Article 11 comes from Japan. Article 120*bis*, prohibits by criminal penalty the manufacture, importation, or public offer of any device, kit to assemble a device, or computer program "having a principal function for the circumvention of technological protection measures."[92] The stat-

---

[87] *See Lasercomb America, Inc.*, 911 F.2d at 979.

[88] *See Eastman Kodak Co.*, 504 U.S. at 451-453 (holding that including anticompetitive clauses in a standard licensing agreement is a misuse of a copyright).

[89] *See id.* at 978-79.

[90] 166 F.3d 772 (5th Cir 1999).

[91] *Id.* at 793 (quoting Lasercomb America, Inc. v. Reynolds, 911 F.2d 970,976 (4th Cir. 1990)).

[92] *See* Copyright Law, Law No. 101 of 1998, art 120*bis*, no. i., *available at* http://clea.wipo.int/lpbin/lpext.dll/clea/LipEN/25b4b/2709b?f=file[document.htm] (last visited April 15, 2002).

ute defines technological protection measures broadly, including all "measures to prevent or deter such acts as constitute infringements on moral rights or copyright... or neighboring rights."[93] Circumvention is defined as "enabl[ing] . . . acts prevented by technological protection measures or to [ceasing] obstruction to the results of acts deterred by such measures, by removal or alteration of signals used for such measures."[94] The removal or alteration of a signal necessitated by conversion between recording or transmission systems does not constitute circumvention under this statute.[95] Article 120*bis* further prohibits any business from offering circumvention of technological protection measures to the public as a service.[96]

Perhaps the most laudable feature of this provision is its limitation of the scope of the statute to devices and computer programs. Unlike the U.S. statute, which encompasses technologies and parts thereof, the Japanese statute requires a tangible circumvention measure to find liability. No reasonable interpretation of the Japanese statute could broaden it to encompass the dissemination of the results of cryptographic research. Although some programmers might balk at the "program" provision, claiming that source code is a necessary means of expressing cryptographic findings,[97] on the whole, the law protects expression in that area quite nicely.

The Japanese statute also differs from the DMCA in its refusal to simply prohibit the circumvention of a technological protection measure. Researchers can freely circumvent measures, so long as they do not manufacture devices based upon the results. It even appears that programs written to circumvent technological protection measures are not forbidden under the statute, so long as they are not distributed. Although the English translation of the statute is a poor vehicle for attempting fine shades of distinction, the statute forbids the manufacture and importation of *copies* of a program.[98] This implies that the prohibited manufacturing activity would involve the reproduction of a successful program, not its original creation. Regardless of whether this is an accurate reflection of Japanese law, including such a distinction in a revised U.S. law would be helpful in encouraging legitimate cryptographic research.

---

[93] *Id.* art. 2(1)(xx).

[94] *Id.* art. 30(1)(ii).

[95] *See id.*

[96] *Id.* art. 120*bis* (ii).

[97] *See* Universal City Studios, Inc. v. Reimerdes, Inc., 111 F. Supp. 2d 294, 305-06 (S.D.N.Y. 2000).

[98] *See* Copyright Law, Law No. 101 of 1998, art 120*bis*, no. i., *available at* http://clea.wipo.int/lpbin/lpext.dll/clea/LipEN/25b4b/2709b?f=file[document.htm] (last visited April 15, 2002).

Finally, the Japanese statute may provide an answer to the over-expansion of the copyright monopoly discussed above. The Japanese provision bans the distribution of devices whose primary purpose is to circumvent technological protection measures in the course of enabling acts prevented by the statute. Since the legitimate owner of a copy of a copyrighted work generally has the right to use that copy, a device, such as a CD or DVD player, that merely allows access to the work does not have the primary purpose of circumventing protections under the statute. By this reasoning, a manufacturer could legally reverse engineer the technological protections in a licensed playback device so long as she complied with all other applicable laws. She could then manufacture a playback device of her own and distribute it, so long as it did not operate to make additional copies of a work or otherwise facilitate copyright infringement. This system eliminates much of the overbreadth of copyright under the DMCA.

B. Prevent the Distribution of Decryption Devices Incapable of Substantial Non-Infringing Uses Under the Doctrine of Contributory Infringement

While the Japanese statute does an admirable job of limiting the scope of the copyright monopoly, it still fails to address the basic problem of paracopyright statutes, as they do not focus on infringement. By creating rights incident to a copyright, paracopyright law imposes the burden of protecting copyrighted works upon the general public. The purpose of Article 11 is to prevent the dissemination of devices and programs to the public that serve no purpose except to facilitate infringement. In the digital environment, these devices have taken the form of the decryption technologies banned by the DMCA, but copyright law has weathered the introduction of new technologies for decades before the Internet. Each time a new technology has arisen, courts have managed to strike a proper balance without the need for paracopyright restrictions. Digital technology is no different; a proper balance can be found in the existing doctrine of contributory infringement.

Under U.S. law, a claim of contributory infringement has three elements.[99] First, there must be an act of direct infringement.[100] Even behavior that is likely to induce or assist an infringing activity is not tortious unless an infringement results.[101] Second, the contributory infringer must either actively induce the act of infringement or pro-

---

[99] *See* PAUL GOLDSTEIN, COPYRIGHT §§ 6.0-6.1 (2d ed. 1996).
[100] *See id.*
[101] *See id.*

vide a product that facilitates such an infringement.[102] Finally, the contributory infringer must have knowledge of the infringing activity.

Where a defendant provides the raw materials for bootleg copies, programs to break into an encrypted file, or devices that facilitate copying, he can substantially aid in the infringing activity without any direct involvement. This makes it difficult to make the requisite showing of knowledge. Even a defendant who intended to profit from the infringing uses of its product may not be aware of a specific infringing activity. If actual knowledge of a specific infringing activity was required, manufacturers of infringing items would maintain a policy of willful blindness, effectively insulating themselves from any liability. Thus, the defendant's knowledge of infringing activity may be assumed where the article is incapable of any substantial non-infringing use.[103]

Application of the contributory infringement doctrine can be problematic, but it allows copyright owners to prevent the dissemination of devices useful mainly for privacy, while avoiding unnecessary encroachments on the public domain. To provide one example, unlike the DMCA, liability under the contributory infringement doctrine, by definition, cannot occur without an actual act of infringement. Secondly, since technologies with substantial non-infringing use are protected under the doctrine, socially useful uses of decryption technology will remain protected. Security testing, encryption research, and similar activities would be excluded without the need for complicated exceptions. Additionally, this standard allows independent manufactures to create devices to utilize the protected material, restricting the copyright monopoly to its intended limits, the protected work.

CONCLUSION

There is no question that stronger copyright protection is necessary given the advances in digital technology. Paracopyright measures such as Article 11 and the DMCA, however, are not an efficient vehicle for policing the use of copyright on digital media. Directly protecting access control measures on copyrighted works chills aca-

---

[102] *See* 35 U.S.C. § 271(b)-(c), *held unconstitutional on other grounds*, (2001) (stating that one is liable for "actively inducing infringement" or offers to sell products that facilitate such infringement).

[103] *See* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 425-27 (1984) (declining to find liability for manufacturer of home video tape recorders ("VTRs") where VTRs had both infringing and non-infringing uses); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020-21 (9th Cir. 2001) (holding that provider of service permitting and facilitating transmission and retention of digital audio files by its users was liable because it had "actual knowledge that *specific* infringing material is available using its system").

demic speech in the field of encryption and grants too great an expansion of the copyright monopoly at the expense of the public. Properly applied, existing law in the field of contributory infringement law is sufficient to protect the interests of copyright holders even considering the increasing ease with which information can be transferred. Failing a return to the contributory infringement approach, an revision of the DMCA to adopt an anti-circumvention provision similar to Japan's would reduce much of its encroachment into the public domain without reducing its effectiveness in protecting copyrighted works.

Copyright is a bargain, between the public and our authors, artists, and musicians. We give up a portion of our freedom to induce them to enrich the public discourse with their creations. Paracopyright provisions such as Article 11 and the DMCA shift the terms of this bargain away from its original balance. They place a greater burden on the public without generating a corresponding benefit. As difficult as it must be to protect one's works in an age where information can circumscribe the globe in seconds, there has to be a better way.

BRIAN BOLINGER[†]

† I would like to thank Professor David Carney, both for sparking my interest in copyright law and for rekindling my interest in law generally, the staff of the Case Western Law Review for their support, and my family, for their patience throughout the writing of this Note.